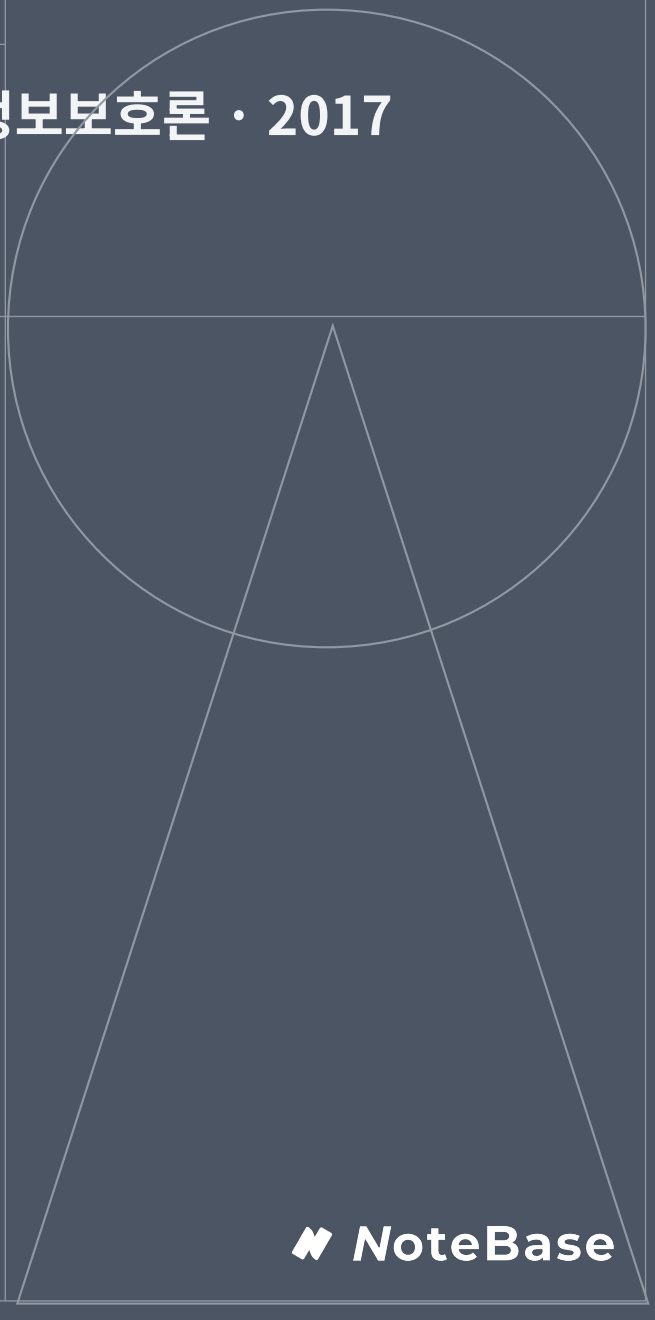
기출OX 해설집

공무원/경찰/공채(경위) · 정보보호론 · 2017



NoteBase

기출OX 해설집

공무원/경찰/공채(경위) · 정보보호론 · 2017

공무원/경찰/공채(경위) · 정보보호론 · 2017

문 1. 다음 지문에서 설명하는 기법은 무엇인가?

가. 그림 또는 문장 속에 비밀자료를 숨겨서 전달하는 방법
나. 그림의 픽셀 중 일부를 저장하고 싶은 데이터로 대체하여 저장하는 방법
다. 원본 그림과 대체된 그림을 육안으로 봐서는 구별할 수 없다.

① 전자서명(Digital Signature)
② 인증서(Certificate)
③ 스테가노그래피(Steganography)
④ 제로데이 공격(Zero-Day Attack)

정답 3번

간단한 해설

스테가노그래피는 그림·문장 같은 평범한 자료 안에 정보를 삽입하여 **비밀정보가 전달되고 있다는 사실 자체를 숨기는** 기법이다. 픽셀을 조금 바꾸어 정보를 넣되 겉보기 차이는 알아채기 어렵게 하는 것이 지문의 핵심 단서이다.

NoteBase

핵심 풀이

스테가노그래피는 다른 자료를 운반 매체로 삼아 비밀정보를 감추는 기법이다. 내용을 읽기 어렵게 바꾸는 암호화와 달리 **숨겨진 정보의 존재를 알아채기 어렵게**하는 데 초점을 둔다.

가. 그림이나 문장 안에 비밀자료를 넣어 전달한다는 설명은, 겉으로 보이는 자료와 실제 전달하려는 정보를 구분한다는 뜻이다. 일반 자료가 비밀정보를 운반하는 매체가 된다.

나·다. 그림의 일부 픽셀 값을 비밀 데이터에 맞추어 조금씩 바꾸면 정보가 이미지 안에 포함된다. 이때 시각적 변화를 작게 만들면 원본과 삽입된 이미지를 육안으로 구별하기 어렵다. 즉 **정보를 삽입하면서도 겉모습은 비슷하게 유지**하는 방식이다.

전자서명은 서명자의 확인과 데이터의 위·변조 탐지에 사용된다. 그림에 비밀정보의 존재를 감추어 넣는 기법을 뜻하지 않는다.

인증서는 공개키와 그 소유자의 신원 등을 연결하여 확인할 수 있도록 하는 전자적 증명이다. 지문의 픽셀 변경과는 목적이 다르다.

제로데이 공격은 알려지지 않았거나 대응이 마련되지 않은 취약점을 이용하는 공격을 가리킨다. 다른 자료 안에 데이터를 숨기는 방식의 명칭은 아니다.

따라서 세 단서가 설명하는 기법은 스테가노그래피이며, ③에 해당한다.

NoteBase

문 2. Diffie-Hellman 알고리즘은 비밀키를 공유하는 과정에서 특정 공격에 취약할 가능성이 존재한다. 이러한 취약점을 이용하여 공격하는 방법은 무엇인가?

① DDoS(Distributed Denial of Service) 공격

② 중간자 개입(Man-In-The-Middle) 공격

③ 세션 하이재킹(Session Hijacking) 공격

④ 강제지연(Forced-Delay) 공격

정답 2번

간단한 해설

기본 Diffie-Hellman 키 교환은 교환한 공개값이 **실제 상대방이 보낸 것인지 인증하지 않는다**. 공격자가 양쪽의 공개값을 자신의 것으로 바꾸면 각 사용자와 서로 다른 비밀키를 공유하여 중간에서 통신에 개입할 수 있다.

핵심 풀이

Diffie-Hellman은 통신 당사자가 공개값을 교환하여 공통 비밀키를 만드는 방법이다. 그러나 인증을 결합하지 않은 기본 방식은 공개값을 보낸 주체의 신원을 확인하지 못한다. 따라서 수동적인 도청에 대한 안전성과 상대방의 신원 인증을 구별해야 한다.

중간의 공격자는 A가 B에게 보내는 공개값과 B가 A에게 보내는 공개값을 가로채 각각 자신의 공개값으로 바꾼다. 그러면 A는 공격자와 하나의 비밀키를, B는 공격자와 다른 비밀키를 공유하면서도 서로 직접 키를 공유했다고 오인한다. 공격자는 **양쪽과 별도로 공유한 키**를 이용해 메시지를 읽고 다시 암호화하여 전달할 수 있다. 원래 두 사용자의 비밀값을 수학적으로 풀어낼 필요는 없다.

이 취약점은 키 교환에 사용되는 공개값을 전자서명 등으로 검증하여 상대방의 신원과 결합하는 방식으로 막아야 한다. 단순히 비밀키가 만들어졌다는 사실만으로 통신 상대가 인증된 것은 아니다.

DDoS 공격은 많은 요청 등으로 서비스 가용성을 떨어뜨리는 공격이고, 세션 하이재킹은 이미 성립한 세션의 식별정보 등을 탈취해 세션을 차지하는 공격이다. 강제지연 공격은 메시지 전달을 의도적으로 늦추는 방식이므로, 공개값을 대체하여 두 개의 키 교환을 만드는 이 사례와 구별된다.

따라서 해당 공격은 **중간자 개입(Man-In-The-Middle) 공격**이며, 선택지 ②와 일치한다.

NoteBase

문 3. 다음 중 암호화 키와 복호화 키가 서로 다른 암호화 알고리즘은 무엇인가?

① DES 알고리즘

② IDEA 알고리즘

③ AES 알고리즘

④ RSA 알고리즘

정답 4번

간단한 해설

RSA는 서로 다른 공개키와 개인키를 한 쌍으로 사용하는 비대칭키 암호이다. DES·IDEA·AES는 송신자와 수신자가 비밀키를 공유하는 대칭키 암호이다.

개념 구분

암호화·복호화에 쓰는 키의 관계로 대칭키 암호와 비대칭키 암호를 구분한다. 여기서 키가 다르다는 것은 알고리즘 내부의 라운드 키나 처리 순서가 다르다는 뜻이 아니라, **공개키와 개인키라는 서로 다른 키를 사용**한다는 뜻이다.

RSA: 비대칭키 암호이다. 기밀성을 위한 암호화에서는 수신자의 공개키로 암호화하고, 그와 짝을 이루는 수신자의 개인키로 복호화한다. 두 키는 수학적으로 관련되어 있지만 서로 같지 않으며, 공개키로부터 개인키를 쉽게 구할 수 없도록 구성한다.

DES: 대칭키 블록 암호이다. 암호화와 복호화에 같은 비밀키를 사용하며, 복호화 과정에서 라운드 키의 적용 순서를 역순으로 바꾸더라도 비대칭키 방식이 되는 것은 아니다.

IDEA: 대칭키 블록 암호이다. 하나의 공유 비밀키를 바탕으로 암호화와 복호화에 필요한 서브키를 구성한다. 복호화용 서브키에 역원 등 다른 값이 쓰일 수 있지만, 공개키·개인키 쌍을 사용하는 구조는 아니다.

AES: 대칭키 블록 암호이다. 양쪽이 공유한 같은 비밀키를 바탕으로 암호화와 복호화를 수행하며, 복호화 때 역변환을 수행한다는 점은 키 체계가 비대칭이라는 뜻이 아니다.

따라서 암호화 키와 복호화 키가 서로 다른 공개키 방식에 해당하는 것은 **RSA인 ④**이다.

NoteBase

문 4. AES 알고리즘에 관한 설명 중 옳지 않은 것은 무엇인가?

① AES는 128, 192, 256비트 키를 사용하고 키 크기에 따라 각각 10, 12, 14 라운드를 갖는다.

② 마스터 키의 크기가 달라도 라운드 키는 모두 128비트이다.

③ AES는 바이트 기반 암호이다.

④ 안전성을 보장하기 위하여 AES는 모든 라운드에 대치, 치환, 뒤섞음, 키덧셈의 네 종류 변환을 사용한다.

정답 4번

간단한 해설

AES의 **마지막 라운드에서는 MixColumns가 생략**된다. 따라서 모든 라운드에서 대치·치환·뒤섞음·키덧셈의 네 변환을 수행한다는 설명은 틀리다.

선지별 해설

AES는 128비트 블록을 처리하는 대칭키 블록 암호이다. 일반 라운드에서는 바이트 대치(SubBytes), 행 이동(ShiftRows), 열 혼합(MixColumns), 라운드 키 덧셈(AddRoundKey)을 수행하지만 마지막 라운드는 구성이 다르다.

① O: AES의 키 길이는 128·192·256비트이며, 라운드 수는 각각 **10·12·14회**이다. 키가 길어지면 키 확장과 라운드 수가 달라지지만 블록 크기는 128비트로 유지된다.

② O: 라운드 키는 128비트 상태와 XOR하는 데 사용하므로 키 원본의 길이와 관계없이 **각 라운드 키는 128비트**이다. 192비트나 256비트 키도 키 확장을 거쳐 라운드마다 필요한 128비트 키를 만든다.

③ O: AES의 128비트 상태는 16바이트로 구성되며 4행 4열의 바이트 배열로 표현된다. SubBytes는 각 바이트를 대치하고 다른 변환도 이 바이트 배열을 대상으로 하므로 바이트 기반 암호라는 설명이 적절하다.

④ X: 마지막 라운드에는 **SubBytes·ShiftRows·AddRoundKey만 수행**하고 MixColumns는 수행하지 않는다. 또한 첫 라운드 전에 초기 AddRoundKey를 적용한다. 따라서 모든 라운드에 네 변환이 들어간다는 ④가 적절하지 않다.

NoteBase

문 5. 다음 중 공개키 암호 시스템의 장점이 아닌 것은 무엇인가?

① 키의 분배가 용이하다.

② 사용자의 증가에 따라 관리할 키의 개수가 상대적으로 적다.

③ 암호화 및 복호화가 빠르다.

④ 키 변화의 빈도가 적다.

정답 3번

간단한 해설

공개키 암호는 큰 수에 대한 연산 등을 사용하므로 일반적으로 **대칭키 암호보다 암·복호화 속도가 느리다**. 따라서 빠른 처리는 공개키 암호의 장점으로 볼 수 없다.

선지별 해설

공개키 암호는 공개해도 되는 공개키와 소유자만 보관하는 개인키의 쌍을 사용한다. 대칭키 암호와 비교할 때 키의 전달·관리에는 유리하지만, 일반적으로 대량 데이터의 암·복호화 연산 부담은 더 크다.

① O: 상대에게 공개키를 알려 주는 데 비밀 통로가 반드시 필요한 것은 아니므로 **비밀키를 직접 공유하는 부담**을 줄일 수 있다. 다만 받은 공개키가 실제 상대의 것인지 확인하는 인증은 필요하다.

② O: 사용자마다 공개키·개인키 한 쌍을 두면 되므로 사용자 수 N에 대해 기본 키 수는 2N개로 선형적으로 증가한다. 모든 사용자 쌍이 서로 다른 대칭키를 직접 공유하는 방식은 $\frac{N(N-1)}{2}$개의 키가 필요하므로, 사용자가 많아질수록 공개키 방식의 키 관리 규모가 상대적으로 작다.

③ X: 일반적인 공개키 암호 연산은 **대칭키 암호보다 느리다**. 그래서 실제 데이터는 빠른 대칭키로 암호화하고 공개키 방식은 그 키의 전달이나 설정 등에 활용하는 혼합 방식이 많이 쓰인다. 빠른 대량 데이터 처리는 공개키 방식 자체의 장점이 아니다.

④ O: 이 문항의 통상적인 비교에서는 장기 공개키·개인키 쌍을 유지한 채 여러 상대와 통신할 수 있어, 세션마다 사용하는 대칭키에 비해 키 변경 부담이 작다는 뜻이다. **상대가 바뀔 때마다 자기 키 쌍을 새로 만들 필요는 없다**. 다만 실제 키 교체 주기는 키의 용도·노출 위험·보안 정책에 따라 정해지며, 모든 공개키가 항상 오래 유지되는 것은 아니다.

NoteBase

문 6. 다음 중 전자서명(Digital Signature)에 대한 설명으로 가장 옳지 않은 것은 무엇인가?

① 인증(Authentication) 기능을 제공하며 개인키로 암호화된 메시지를 제3자의 공개키로 복호화 할 경우 메시지를 읽을 수 없다.

② 비밀성(Confidentiality) 기능을 제공하며 대칭키 암호화 알고리즘을 이용하여 전자서명을 생성할 수 있다.

③ 무결성(Integrity) 기능을 제공하며 메시지의 부분 또는 전체를 바꿀 경우 복호화된 메시지를 통해 변경 여부를 확인할 수 있다.

④ 부인방지(Non-Repudiation) 기능을 제공하며 송신자의 개인키와 공개키를 가지고 암호화와 복호화하여 저장된 메시지를 생성할 수 있다.

정답 2번

간단한 해설

전자서명은 **인증·무결성·부인방지**에 사용되며, 메시지 내용을 감추는 비밀성은 별도의 암호화로 확보한다. 전자서명의 생성과 검증에는 **개인키·공개키 쌍**을 사용한다.

선지별 해설

① O: 전자서명은 서명자의 신원을 확인하는 인증에 사용된다. 서명자의 개인키로 만든 서명은 **그 개인키에 대응하는 공개키**로 검증해야 하므로, 관계없는 제3자의 공개키로는 올바르게 검증할 수 없다. 선지의 암호화·복호화는 서명 생성·검증을 단순화한 표현이다.

② X: 전자서명은 인증·무결성·부인방지를 제공하지만, 메시지 내용을 숨기는 **비밀성을 자체적으로 제공하지 않는다**. 또한 서명은 비대칭키 방식으로 생성·검증한다. 대칭키를 공유하는 메시지 인증 코드와 구별해야 하며, 내용을 비밀로 유지하려면 별도의 암호화가 필요하다.

③ O: 서명 검증에서는 수신한 메시지와 서명의 대응을 확인한다. 일반적으로 메시지의 해시값을 서명 검증에 사용하므로, 메시지가 일부라도 바뀌면 검증이 실패하여 **변경 여부를 탐지**할 수 있다. 이는 내용을 복원하는 기능이 아니라 위·변조를 확인하는 무결성 기능이다.

④ O: 송신자는 자신의 개인키로 서명을 생성하고, 검증자는 송신자의 공개키로 이를 검증한다. 메시지와 서명을 보관하면 나중에도 작성 주체를 확인하는 증거로 사용할 수 있으므로 **송신자의 서명 사실 부인 방지**를 지원한다. 이때 개인키의 안전한 관리와 공개키 소유자 확인이 전제되며, 단순히 메시지를 저장했다는 사실만으로 부인방지가 성립하는 것은 아니다.

NoteBase

문 7. 다음 중 로봇프로그램과 사람을 구분하는 방법의 하나로 사람이 인식할 수 있는 문자나 그림을 활용하여 자동 회원가입 및 게시글 포스팅을 방지하는데 사용하는 방법은 무엇인가?

① 해시함수(Hash Function)

② 인증서(Certificate)

③ 전자서명(Digital Signature)

④ 캡차(CAPTCHA)

정답 4번

간단한 해설

CAPTCHA는 사람이 수행할 수 있는 인식 과제로 자동화 프로그램의 접근을 걸러내는 방법이다. 문제의 문자·그림 판별은 대량 자동 회원가입이나 게시글 등록을 줄이기 위한 대표적인 CAPTCHA 방식이다.

개념 구분

결정적인 단서는 '사용자가 누구인가'가 아니라 **사람이 수행하는 요청인지 자동화 프로그램의 요청인지 구분**한다는 목적이다. 문자나 그림을 보고 답하게 하는 과제를 통해 자동 처리를 어렵게 한다.

CAPTCHA: 사람은 비교적 쉽게 풀지만 자동화 프로그램은 처리하기 어렵도록 설계한 과제를 제시한다. 왜곡된 문자를 읽거나 특정 그림을 선택하게 하는 방식이 그 예다. 자동 회원가입·스팸 게시를 줄이기 위한 수단이며, 모든 봇을 완벽히 차단하거나 사용자의 실명을 확인한다는 뜻은 아니다.

해시함수: 입력 데이터를 일정한 길이의 해시값으로 변환한다. 데이터의 변경 여부를 검사하는 데 활용할 수 있지만, 해시값 계산 자체로 요청자가 사람인지 봇인지 판별하지는 못한다.

인증서: 인증기관의 전자서명 등을 통해 공개키와 그 소유자의 식별정보 사이의 연결을 확인하는 전자 문서이다. 공개키의 주체를 확인하는 데 쓰이며, 문자·그림 과제로 사람과 프로그램을 가르는 방법은 아니다.

전자서명: 서명자의 개인키로 생성하고 대응하는 공개키로 검증하여 문서의 무결성과 서명 주체의 진정성을 확인하는 수단이다. 자동화 프로그램도 키를 가지고 서명을 생성할 수 있으므로, 서명 여부만으로 사람의 직접 입력을 확인하지는 못한다.

따라서 문제에서 설명하는 방법은 **CAPTCHA인 ④**이다.

NoteBase

문 8. 다음 중 공인인증서의 설명으로 옳지 않은 것은 무엇인가?

① 공인인증서는 사용자의 공개키와 사용자의 ID정보를 결합하여 인증기관의 전자서명을 포함한 문서이다.

② 공인인증서에는 버전, 발행자, 유효기간, 알고리즘 식별자, 사용자의 개인키 등이 포함되어 있다.

③ 인증기관이 자신의 키를 이용하여 전자서명을 생성 후, 인증서에 첨부하고, 인증기관 키를 사용하여 인증서의 유효성을 확인한다.

④ 공인인증서 관련한 표준으로 X.509가 있으며 대부분의 인증서는 이 표준을 따르고 있다.

정답 2번

간단한 해설

인증서는 사용자의 신원과 **공개키**를 연결해 증명하는 문서이다. 공개되는 인증서에 사용자가 비밀로 보관해야 할 개인키를 넣는다는 설명은 옳지 않다.

선지별 해설

① O. 인증서는 사용자 식별 정보와 그 사용자의 공개키를 연결하고, 그 연결을 인증기관의 전자서명으로 보증한다. 수신자는 신뢰하는 인증기관의 서명을 확인하여 공개키의 소유자를 판단할 수 있다.

② X. 인증서에는 버전, 발행자, 유효기간, 알고리즘 식별자와 사용자의 **공개키** 등이 들어간다. 개인키는 사용자만 비밀로 보관해야 하므로 인증서에 포함되는 정보가 아니다. 따라서 '사용자의 개인키'를 '사용자의 공개키'로 고쳐야 한다.

③ O. 인증기관은 자신의 **개인키로 서명**하고, 검증자는 인증기관의 **공개키로 그 서명을 검증**한다. 선지의 '인증기관 키'는 두 단계에서 역할이 다른 이 키 쌍을 가리킨다. 서명 검증은 인증서 검증의 핵심이며, 실제 사용 시에는 유효기간과 폐지 여부 등도 함께 확인한다.

④ O. X.509는 공개키 인증서의 형식을 정한 표준이다. 사용자와 발행자의 식별 정보, 유효기간, 사용자 공개키 및 인증기관의 서명 등을 정해진 구조로 표현한다.

개인키를 인증서의 구성 정보로 제시한 ②가 옳지 않은 설명이다.

NoteBase

문 9. 디스크 스케줄링 정책 중 큐의 항목을 순차적으로 처리하는 것은 무엇인가?

① SSTF(Shortest Service Time First)

② FIFO(First-In-First-Out)

③ SCAN

④ C-SCAN(Circular SCAN)

정답 2번

간단한 해설

FIFO는 먼저 큐에 들어온 요청을 먼저 처리하므로 요청이 들어온 순서를 그대로 따른다. 디스크 헤드와의 거리나 이동 방향에 맞추어 요청 순서를 다시 정하지 않는다는 점이 구별 기준이다.

개념 구분

발문의 '큐의 항목을 순차적으로 처리'는 대기 큐에 들어온 순서대로 서비스한다는 뜻이다. 어떤 트랙이 더 가까운지보다 **요청의 도착 순서**가 우선하는 정책을 찾으면 된다.

FIFO(FCFS): 가장 먼저 도착하여 큐의 앞에 있는 요청부터 처리한다. 예를 들어 요청이 A, B, C 순서로 들어오면 헤드와의 거리에 관계없이 A → B → C 순서로 처리한다. 도착 순서를 바꾸지 않는 것이 핵심이다.

SSTF: 현재 헤드 위치에서 서비스에 필요한 이동 시간이 가장 짧은 요청을 우선한다. 통상 현재 위치와 가장 가까운 트랙의 요청을 선택하므로, 나중에 들어온 요청이 먼저 처리될 수 있다. 따라서 도착 순서대로 처리하는 FIFO와 다르다.

SCAN: 헤드가 한쪽 방향으로 이동하며 지나가는 트랙의 요청을 처리하고, 디스크 끝에 도달하면 방향을 바꾸어 반대쪽 요청을 처리한다. 서비스 순서는 큐에 들어온 순서보다 헤드의 현재 이동 방향과 트랙 위치에 영향을 받는다.

C-SCAN: 헤드가 한 방향으로 이동할 때만 요청을 처리한다. 한쪽 끝에 도달하면 반대쪽 끝으로 돌아간 뒤 같은 방향의 처리를 다시 시작하며, 돌아가는 구간에서는 요청을 처리하지 않는다. 이 역시 도착 순서를 그대로 따르는 방식은 아니다.

따라서 큐에 들어온 순서대로 처리하는 정책은 **FIFO인** ②이다.

NoteBase

문 10. 컴퓨터의 메모리는 사용되는 방식에 따라 여러 개의 영역으로 나누어 생각할 수 있는데 프로그램 실행 중 malloc()등의 system call로 할당되어 사용되다가 free()등의 system call로 해제되는 영역은 무엇인가?

① Text 영역

② Data 영역

③ Stack 영역

④ Heap 영역

정답 4번

간단한 해설

malloc()로 실행 중 필요한 메모리를 확보하고 free()로 반환하는 방식은 **동적 메모리 할당**이다. 프로그램의 메모리 영역 구분에서는 이러한 공간을 Heap 영역으로 본다.

개념 구분

Heap 영역: 실행 중 필요한 크기의 메모리를 동적으로 확보하고 반환하는 영역이다. malloc()는 요청한 메모리 블록의 주소를 돌려주고 free()는 그 동적 할당 블록을 해제한다. **함수 호출이 끝났다는 이유만으로 해당 블록이 자동 해제되지는 않는다**는 점이 Stack과 다르다.

Text 영역: 프로그램이 실행할 기계어 명령 등이 저장되는 코드 영역이다. malloc()로 확보한 데이터 블록을 두는 영역을 뜻하지 않는다.

Data 영역: 전역 변수와 정적 변수처럼 프로그램 실행 동안 유지되는 데이터를 위한 영역이다. 세부 구분에서는 초기화되지 않은 정적 데이터를 BSS 영역으로 나누기도 한다. 필요한 시점마다 malloc()로 확보하는 공간과는 다르다.

Stack 영역: 함수의 호출·복귀 정보와 일반적인 자동 지역 변수 등을 관리한다. 호출 흐름에 따라 사용 공간이 늘고 줄며, **명시적으로 할당·해제하는 동적 블록**인 Heap과 구별된다.

용어 구별: 발문은 malloc()와 free()를 system call이라고 표현했지만, 엄밀히는 C 라이브러리 함수이다. 메모리 관리 구현은 필요에 따라 운영체제의 시스템 호출을 이용할 수 있다. 이 명칭 차이와 관계없이 문제의 핵심은 실행 중 동적 할당·해제이다.

따라서 해당 영역은 ④ Heap 영역이다.

NoteBase

문 11. 유닉스(Unix) 운영체제에서 파일에 대한 권한을 모두 허용 (-rwxrwxrwx)하는 모드(명령어)는 무엇인가?

① chmod 777

② chmod a-rwx

③ chmod 666

④ chmod ug+rw

정답 1번

간단한 해설

읽기 r · 쓰기 w · 실행 x의 권한값은 각각 4 · 2 · 1이므로 **rwx는 4 + 2 + 1 = 7**이다. 소유자 · 그룹 · 기타 사용자 모두 rwx를 부여하려면 세 자리를 **777**로 지정한다.

계산 과정

권한 표시 '-rwxrwxrwx'에서 맨 앞의 '-'는 일반 파일이라는 뜻이다. 그 뒤의 아홉 글자는 소유자 u, 그룹 g, 기타 사용자 o의 권한을 세 글자씩 나타낸다. 따라서 요구된 권한은 세 대상 모두 rwx이다.

각 대상의 권한은 읽기 r=4, 쓰기 w=2, 실행 x=1을 더하여 8진수 한 자리로 표시한다. rwx의 값은 4 + 2 + 1 = 7이다.

소유자 권한이 rwx이므로 첫 자리는 7, 그룹 권한이 rwx이므로 둘째 자리는 7, 기타 사용자 권한도 rwx이므로 셋째 자리는 7이다. 따라서 전체 모드는 **777**이 된다.

'chmod a-rwx'는 모든 대상의 읽기 · 쓰기 · 실행 권한을 제거한다.

'chmod 666'은 각 대상에게 읽기와 쓰기만 부여하여 실행 권한이 없다.

'chmod ug+rw'는 소유자와 그룹에 읽기 · 쓰기를 추가하는 상대적 변경이며, 기타 사용자의 권한과 실행 권한을 모두 허용하도록 지정하는 명령은 아니다.

세 대상 모두에게 읽기 · 쓰기 · 실행 권한을 지정하는 것은 'chmod 777'이므로 ①과 일치한다.

NoteBase

문 12. 리눅스(Linux) 사용자의 패스워드를 암호화하여 저장하고 있는 파일은 무엇인가?

① /etc/shadow

② /etc/passwd

③ /etc/skel

④ /etc/group

정답 1번

간단한 해설

일반적인 shadow 패스워드 방식에서는 **/etc/shadow에 사용자 비밀번호의 해시값**을 저장한다. 공개적으로 읽을 수 있는 /etc/passwd와 분리하여 비밀번호 검증 정보에 대한 접근을 제한한다.

개념 구분

리눅스의 일반적인 shadow 패스워드 방식은 계정 정보와 비밀번호 검증 정보를 서로 다른 파일에 저장한다. 문제의 '암호화하여 저장'은 통상 비밀번호를 그대로 보관하지 않고 **일방향 해시 등으로 변환한 검증값을 저장**한다는 의미이다. 로그인할 때 원래 비밀번호를 복호화하여 꺼내는 방식이 아니다.

/etc/shadow: 계정별 비밀번호 해시와 마지막 변경일, 만료 기간 등의 비밀번호 관리 정보를 저장한다. 일반 사용자가 읽지 못하도록 접근 권한을 제한한다. 잠기거나 비밀번호 인증이 비활성화된 계정에는 해시 대신 잠금 표시 등이 들어갈 수도 있다.

/etc/passwd: 사용자 이름, UID, GID, 홈 디렉터리, 로그인 셸 등 기본 계정 정보를 저장한다. shadow 방식을 사용할 때 비밀번호 필드에는 보통 x를 두고, 실제 비밀번호 검증 정보는 /etc/shadow에 분리한다. 이 x가 비밀번호의 해시값이라는 뜻은 아니다.

/etc/skel: 새 사용자 홈 디렉터리를 만들 때 복사할 초기 설정 파일을 모아 둔 디렉터리이다. 계정 생성의 기본 환경을 제공하며, 사용자 비밀번호를 저장하는 파일이 아니다.

/etc/group: 그룹 이름, GID, 그룹 구성원 등 그룹 정보를 저장한다. 사용자별 로그인 비밀번호의 해시를 보관하는 /etc/shadow와 역할이 다르다.

따라서 비밀번호 검증 정보를 저장하는 파일은 **/etc/shadow인 ①**이다.

NoteBase

문 13. 윈도우(Windows)에서 지원하지 않는 파일시스템은 무엇인가?

① FAT32

② EXT2

③ NTFS

④ FAT16

정답 2번

간단한 해설

EXT2는 **리눅스 계열 파일시스템**으로, 이 문항에서 묻는 윈도우의 기본 지원 대상과 구별된다.
FAT16·FAT32·NTFS는 윈도우에서 지원한다.

개념 구분

FAT32: 윈도우가 기본 지원하는 FAT 계열 파일시스템이다. 파일 할당표를 이용해 파일에 배정된 저장 공간을 관리한다.

EXT2: 리눅스에서 사용되어 온 확장 파일시스템이며, 이 문항에서 묻는 **윈도우의 기본 지원 파일시스템에 포함되지 않는다**. 별도 드라이버 등을 추가하여 접근하는 경우와 운영체제의 기본 지원은 구분한다.

NTFS: 윈도우 NT 계열에서 사용되는 대표적인 파일시스템이다. 파일·폴더의 접근 권한 등 보안 기능을 제공한다.

FAT16: FAT32보다 앞서 사용된 FAT 계열 파일시스템으로, 윈도우에서 호환성을 위해 지원한다.

따라서 윈도우가 기본 지원하지 않는 파일시스템은 EXT2이므로 ②에 해당한다.

NoteBase

문 14. 윈도우(Windows) 시스템의 레지스트리(Registry)에 대한 설명으로 옳지 않은 것은 무엇인가?

① HKEY_CLASSES_ROOT는 시스템에 등록된 파일 확장자와 그것을 열 때 사용할 어플리케이션에 대한 맵핑 정보 등을 갖고 있다.

② HKEY_CURRENT_USER는 시스템이 시작할 때 사용하는 하드웨어 프로파일 정보를 저장하고 있다.

③ HKEY_USERS는 시스템에 있는 모든 계정과 그룹에 관한 정보를 저장하고 있다.

④ HKEY_LOCAL_MACHINE은 시스템에 있는 하드웨어, 소프트웨어 정보를 갖고 있다.

정답 2번

간단한 해설

HKEY_CURRENT_USER는 **현재 로그인한 사용자의 환경 설정**을 담는다. 시스템 시작 시 사용하는 하드웨어 프로파일 정보는 **HKEY_CURRENT_CONFIG**에 해당한다.

출제 포인트

레지스트리의 루트 키를 저장 정보의 대상과 범위에 따라 구분하는 문제이다.

핵심 개념

레지스트리는 Windows의 사용자, 응용 프로그램, 하드웨어 설정을 계층적으로 저장하는 데이터베이스이다.
HKEY_CURRENT_USER는 현재 사용자의 설정, HKEY_USERS는 로드된 사용자 프로파일들의 설정을 담는다.
사용자 프로파일은 화면 색상이나 프로그램 설정처럼 사용자별로 유지하는 환경 정보이다.
HKEY_LOCAL_MACHINE은 컴퓨터 전체에 적용되는 설정, HKEY_CURRENT_CONFIG는 현재 사용하는 하드웨어 프로파일 정보를 담는다.

NoteBase

선지별 해설

① O
HKEY_CLASSES_ROOT는 파일 확장자와 응용 프로그램의 연결 정보를 제공한다. 파일을 열 때 어떤 프로그램을 사용할지 결정하는 데 이 정보가 쓰인다.

② X
'시스템이 시작할 때 사용하는 하드웨어 프로파일 정보'는 HKEY_CURRENT_CONFIG의 설명이다. HKEY_CURRENT_USER의 설명은 '현재 로그인한 사용자의 환경 설정을 저장한다'로 고친다. 화면 색상과 제어판 설정 등이 이에 해당한다.

③ O (이 문항의 정답 처리)
HKEY_USERS는 컴퓨터에 현재 로드된 사용자 프로파일들의 설정을 담으며 HKEY_CURRENT_USER는 그중 현재 사용자에 해당하는 부분을 가리킨다. 다만 선지의 '모든 계정과 그룹'은 엄밀한 표현이 아니다. 모든 계정과 그룹의 정보를 저장하는 곳으로 일반화하지 않고 '로드된 사용자 프로파일들의 설정'으로 이해한다.

④ O
HKEY_LOCAL_MACHINE은 설치된 하드웨어와 소프트웨어 등 컴퓨터 자체의 구성 정보를 담는다. 특정 사용자만의 환경 설정과 달리 컴퓨터 전체에 적용되는 정보를 다룬다.

오답 포인트

②는 이름에 'CURRENT'가 있다는 점을 이용해 사용자 설정과 하드웨어 프로파일을 바꾸어 설명했다. CURRENT 뒤의 USER와 CONFIG를 구분한다. ③의 표현을 모든 보안 계정·그룹 정보의 저장 위치로 확대해 암기하지 않는다.

다시 나오면 이렇게 판단

파일 확장자와 실행 프로그램의 연결은 CLASSES_ROOT, 현재 사용자의 설정은 CURRENT_USER, 로드된 사용자 프로파일들은 USERS로 구분한다. 컴퓨터 전체의 하드웨어·소프트웨어 구성은 LOCAL_MACHINE, 현재 하드웨어 프로파일은 CURRENT_CONFIG에 대응시킨다.

암기 포인트

CURRENT_USER = 현재 사용자 설정 / CURRENT_CONFIG = 현재 하드웨어 프로파일. USERS는 사용자 프로파일, LOCAL_MACHINE은 컴퓨터 전체 설정이다.

NoteBase

문 15. 다음은 윈도우7 운영체제의 명령어 창에서 어떤 명령어를 실행한 출력 결과의 일부이다. 실행한 명령어는 무엇인가?

이미지 이름	PID	세션 이름	세션#	메모리 사용
System Idle	0	Services	0	12 K
Process	4	Services	0	284 K
System	472	Services	0	844 K
smss.exe	592	Services	0	4,672 K
csrss.exe	648	Console	1	16,528 K
csrss.exe	656	Services	0	4,288 K
wininit.exe	708	Services	0	9,260 K
services.exe	732	Services	0	8,900 K
lsass.exe	740	Console	1	6,244 K
winlogon.exe	768	Services	0	4,580 K
lsm.exe	868	Services	0	7,340 K
svchost.exe	928	Services	0	5,780 K
nvvsvc.exe	960	Services	0	6,564 K
svchost.exe	1048	Services	0	3,228 K

① netstat -an

② ipconfig /all

③ tasklist

④ arp -a

정답 3번

간단한 해설

'이미지 이름', 'PID', '메모리 사용'은 **실행 중인 프로세스 목록**의 핵심 열이다. 이 목록을 출력하는 윈도우 명령은 tasklist이다.

NoteBase

도식 해설

제시된 표에는 '이미지 이름', 'PID', '세션 이름', '세션#', '메모리 사용'이 표시되어 있다. smss.exe, csrss.exe, services.exe 등은 실행 중인 프로세스의 이름이며, PID는 각 프로세스를 식별하는 번호이다. 따라서 이 출력은 **실행 중인 프로세스 목록**을 보여 주는 tasklist의 결과이다.

① netstat -an은 네트워크 연결과 수신 대기 포트 등을 주소·포트 번호를 숫자로 표시하여 보여 준다. 제시된 프로세스 목록을 출력하는 명령이 아니다.

② ipconfig /all은 네트워크 어댑터별 IP 주소, 서브넷 마스크, 기본 게이트웨이, DNS 서버, 물리적 주소 등의 상세 설정을 보여 준다.

③ tasklist는 프로세스의 이미지 이름, PID, 세션 정보, 메모리 사용량 등을 표시한다. 제시된 열의 구성과 일치한다.

④ arp -a는 ARP 캐시에 저장된 IP 주소와 물리적 주소(MAC 주소)의 대응 관계 등을 표시한다. 프로세스 이름이나 프로세스별 메모리 사용량을 보여 주는 명령이 아니다.

따라서 제시된 출력 결과를 만드는 명령어는 ③ tasklist이다.

NoteBase

문 16. 유닉스(Unix) 운영체제의 로그파일과 그 로그파일에 기록되는 내용을 바르게 짝지은 것은 무엇인가?

가. history - 각 사용자별 수행한 명령을 기록
나. sulog - su 명령어의 로그를 기록
다. xferlog - 실패한 로그인 시도를 기록
라. loginlog - FTP 파일 전송 내역을 기록

① 가, 나
② 가, 다
③ 나, 다
④ 다, 라

정답 1번

간단한 해설

history는 사용자별 명령 이력을, sulog는 su 명령 사용 내역을 기록한다. **xferlog는 FTP 전송 기록**, **loginlog는 로그인 실패 기록**이므로 다와 라는 기록 대상을 서로 바꾸었다.

보기별 해설

로그의 이름보다 기록하는 행위를 기준으로 구별한다. 명령 실행 이력, 사용자 전환, 파일 전송, 로그인 실패는 서로 다른 기록 대상이며, 실제 저장 위치나 활성화 조건은 운영체제와 셸 설정에 따라 달라질 수 있다.

가. O: history는 사용자가 셸에서 입력한 명령의 이력이다. 셸은 사용자별 명령 목록을 유지하고 설정에 따라 이력 파일에 저장하므로 **사용자별 수행 명령을 기록**한다는 연결이 적절하다.

나. O: sulog는 su 명령으로 다른 사용자 권한으로 전환하려는 시도와 관련된 기록이다. 사용자 전환의 성공·실패 등을 남기므로 **su 명령어의 로그**라는 연결이 적절하다. root로 전환하는 경우에만 한정되는 기록은 아니다.

다. X: xferlog는 **FTP 파일 전송 내역**을 기록한다. 전송된 파일, 전송 시각과 전송량 등의 정보를 다루며, 로그인 실패 기록이라는 설명은 loginlog와 바뀌었다.

라. X: loginlog는 **실패한 로그인 시도**를 기록하는 로그이다. FTP 파일 전송 내역은 xferlog에 해당하므로 기록 대상을 바로잡아야 한다.

바르게 연결된 항목은 가와 나이므로 ①과 일치한다.

NoteBase

문 17. 다음 지문에서 설명하는 공격은 무엇인가?

가. 두 프로세스 간 자원 사용에 대한 경쟁을 이용하여 시스템 관리자의 권한을 획득하고, 파일에 대한 접근을 가능하게 하는 공격 기법
나. 공격 조건으로 프로그램에 root권한의 SetUID가 설정되어야 함
다. 대응 방법으로는 임시파일 사용 시 링크상태, 파일의 종류, 파일의 소유자, 파일의 변경여부 등을 점검

① 힙 오버플로우(Heap Overflow) 공격
② 레이스 컨디션(Race Condition) 공격
③ 스택 오버플로우(Stack Overflow) 공격
④ 코드(Code) 기반 공격

정답 2번

간단한 해설

프로세스 간 자원 사용 경쟁과 **검사 시점·사용 시점 사이의 상태 변화**를 악용하는 것이 레이스 컨디션 공격이다. 관리자 권한으로 실행되는 프로그램의 파일 처리에 이런 틈이 있으면 권한 없는 파일 접근으로 이어질 수 있다.

NoteBase

핵심 풀이

가. 두 프로세스가 같은 자원을 다루는 동안 **실행 순서나 시점의 차이**를 악용하는 것이 레이스 컨디션 공격이다. 파일을 검사한 뒤 실제로 사용하기 전에 상태가 달라질 수 있는 검사 시점과 사용 시점의 차이도 여기에 해당한다.

나. 지문은 root 소유의 SetUID 프로그램이 관리자 권한으로 실행되는 상황을 전제로 한다. 이 프로그램이 사용하는 파일의 상태를 안전하게 보장하지 못하면 권한 없는 사용자가 관리자 권한의 파일 처리 결과를 악용할 수 있다. 다만 **SetUID는 이 사례의 조건**이며, 모든 레이스 컨디션의 필수 조건은 아니다.

다. 임시파일의 링크 상태·종류·소유자·변경 여부를 확인하는 이유는 의도한 파일과 실제 처리할 파일이 같은지 확인하기 위해서이다. 점검 뒤에도 상태가 바뀔 수 있으므로, 안전한 임시파일 생성과 동기화 등으로 **검사부터 사용까지 자원 상태가 바뀌지 않도록** 해야 한다.

힙 오버플로우는 동적으로 할당된 힙 영역의 버퍼 범위를 넘는 쓰기를 악용한다.

스택 오버플로우는 스택 영역의 버퍼 범위를 넘는 쓰기를 악용한다. 둘 다 이 지문의 자원 사용 시점 경쟁과는 원리가 다르다.

코드 기반 공격이라는 포괄적 표현보다, 프로세스 간 자원 경쟁이라는 구체적 원리를 나타내는 레이스 컨디션이 지문에 부합한다.

따라서 지문이 설명하는 공격은 레이스 컨디션 공격이며, ②에 해당한다.

NoteBase

문 18. OSI 7계층 중 다음 내용을 수행하는 계층은 무엇인가?

가. 메시지 분할 및 조립, 순서화
나. 포트주소 지정
다. 연결제어
라. 다중화와 역다중화

① 전송층(Transport Layer)
② 링크층(Link Layer)
③ 네트워크층(Network Layer)
④ 세션층(Session Layer)

정답 1번

간단한 해설

포트 번호로 응용 프로세스를 구분하고 종단 간 데이터를 전달하는 것은 전송층의 역할이다. 제시된 분할·조립, 연결 제어, 다중화·역다중화도 이 프로세스 간 전달을 위한 기능이다.

NoteBase

핵심 풀이

OSI 전송층은 서로 다른 호스트의 응용 프로세스 사이에 종단 간 데이터 전달 서비스를 제공한다. 여러 기능 중 **포트 주소를 사용한다**는 단서가 전송층을 가장 직접적으로 가리킨다.

가. 메시지 분할 및 조립, 순서화: 송신 측에서 상위 계층의 데이터를 전송에 적합한 단위로 나누고, 수신 측에서 다시 구성한다. TCP와 같은 신뢰성 있는 전송 방식에서는 순서번호를 이용하여 순서를 맞춘다. 네트워크층의 IP 단편화와 혼동하지 않아야 한다.

나. 포트주소 지정: 한 호스트 안에서 통신할 응용 프로세스나 서비스를 구분하기 위해 포트 번호를 사용한다. IP 주소가 주로 어느 호스트로 보낼지를 식별한다면, 포트 번호는 그 호스트 안의 어느 통신 종점으로 전달할지를 구분한다.

다. 연결제어: 연결 지향 전송에서는 데이터 전달에 필요한 전송 연결을 설정하고 유지한 뒤 종료한다. TCP가 그 예다. UDP와 같이 연결을 설정하지 않는 전송 프로토콜도 있으므로, 모든 전송층 프로토콜이 반드시 연결 지향이라는 뜻은 아니다.

라. 다중화와 역다중화: 송신 측은 여러 응용 프로세스의 데이터를 전송층에서 받아 하위 계층으로 넘기고, 수신 측은 포트 등의 정보를 이용하여 데이터를 해당 프로세스에 나누어 전달한다. 여기서 다중화는 물리 신호의 주파수 분할 등이 아니라 여러 프로세스의 통신을 함께 처리하는 기능이다.

링크층은 인접한 노드 사이의 프레임 전달을, 네트워크층은 논리 주소와 경로 선택을 중심으로 한다. 세션층은 응용 간 대화 관리와 동기화 등을 담당한다. 따라서 '연결제어'라는 말 하나만 보고 세션층을 고르지 말고, **포트와 프로세스 간 전달이라는 공통 맥락**을 함께 확인해야 한다.

제시된 기능을 수행하는 계층은 **전송층인 ①**이다.

NoteBase

문 19. 다음은 TCP 제어 플래그에 대한 설명이다. 옳지 않은 것은 무엇인가?

① TCP 제어 플래그는 TCP 연결제어나 전송 데이터를 관리하기 위해 사용된다.

② URG 패킷은 순서에 상관없이 우선적으로 전송된다.

③ SYN 패킷은 TCP 통신에서 세션 확립을 위해 가장 먼저 전송된다.

④ RST 패킷은 송신측에서 더 이상 보낼 데이터가 없을 때 전송된다.

정답 4번

간단한 해설

송신 측이 더 이상 보낼 데이터가 없음을 알리는 플래그는 **FIN**이다. RST는 **연결을 재설정하거나 비정상적으로 끊을 때** 사용한다.

출제 포인트

TCP 제어 플래그의 기능, 특히 정상적인 송신 종료를 알리는 FIN과 연결을 재설정하는 RST를 구분하는 문제이다.

핵심 개념

TCP 제어 플래그는 TCP 헤더에서 연결의 시작·종료나 데이터 처리 상태를 나타내는 비트이다. SYN은 연결 시작과 순서 번호 동기화, FIN은 송신 종료, RST는 연결 재설정에 사용한다. URG는 긴급 포인터가 유효함을 나타내며 수신 측에 긴급 처리가 필요한 데이터를 알린다.

NoteBase

선지별 해설

① O
TCP 제어 플래그는 연결을 설정하거나 종료하고 수신 확인이나 긴급 데이터 처리 등을 제어한다. 따라서 연결 제어와 전송 데이터 관리에 사용된다는 설명은 옳다.

② O
이 문항에서는 '우선적으로 전송된다'를 긴급 데이터의 우선 처리를 가리키는 표현으로 보아 옳게 처리한다. URG는 긴급 포인터가 유효함을 나타내고 수신 응용 프로그램에 긴급 처리 필요성을 알린다. 다만 URG 자체가 네트워크의 패킷 전송 순서를 바꾸거나 TCP의 순서 번호 체계를 없애는 것은 아니다.

③ O
일반적인 TCP 연결 설정은 SYN, SYN+ACK, ACK 순서의 3단계 핸드셰이크로 이루어진다. 연결을 시작하는 쪽이 먼저 SYN을 보내 연결 설정을 요청한다.

④ X
'송신측에서 더 이상 보낼 데이터가 없을 때 전송된다'는 FIN의 기능이다. RST는 연결을 재설정하거나 비정상적으로 끊는 데 사용한다. 따라서 이 설명의 RST를 FIN으로 고쳐야 한다.

오답 포인트

④는 연결을 끝내는 플래그라는 공통점 때문에 FIN과 RST를 혼동하게 한다. '더 이상 보낼 데이터가 없다'는 정상적인 송신 종료의 의미이므로 FIN에 해당한다. ②의 표현은 시험에서 긴급 처리 기능을 간략히 설명한 것으로 이해하되 실제 전송 순서 보장과는 구분한다.

다시 나오면 이렇게 판단

플래그 이름보다 수행하는 기능을 먼저 연결한다. 연결 시작은 SYN, 정상적인 송신 종료는 FIN, 연결 재설정은 RST이다. URG의 '긴급'은 수신 측에 알리는 처리 필요성으로 이해한다.

암기 포인트

SYN: 시작 / FIN: 송신 종료 / RST: 재설정 / URG: 긴급 처리 알림

NoteBase

문 20. 다음 중 프로토콜과 포트번호의 연결이 옳지 않은 것은 무엇인가?

① HTTP - 80

② SMTP - 25

③ DNS - 53

④ TELNET - 20

정답 4번

간단한 해설

TELNET의 표준 포트는 **23번**이다. 제시된 **20번은 FTP 데이터 전송용 포트**이므로 TELNET과의 연결이 잘못되었다.

선지별 해설

포트 번호는 통신 상대의 응용 서비스를 구별한다. 이 문항은 관리자가 임의로 바꾼 설정이 아니라 각 서비스에 통상적으로 대응하는 표준 포트를 묻는다.

① O: HTTP는 웹 문서와 자원을 요청하고 응답하는 프로토콜이며, 기본 포트는 **80번**이다. 따라서 HTTP와 80의 연결이 적절하다.

② O: SMTP는 전자우편을 전달하는 프로토콜이며, 메일 서버 간 전송에 사용하는 표준 TCP 포트는 **25번**이다. 따라서 SMTP와 25의 연결이 적절하다.

③ O: DNS는 도메인 이름에 대응하는 주소 등 이름 정보를 조회하는 서비스이며, 기본 포트는 **53번**이다. DNS는 UDP뿐 아니라 TCP도 사용할 수 있고 두 경우 모두 표준 서비스 포트가 53번이다.

④ X: TELNET은 원격 터미널 접속을 제공하며 표준 TCP 포트는 **23번**이다. 20번은 FTP의 기본 데이터 전송 포트이고, FTP 제어 연결은 21번이다. 따라서 TELNET을 20번과 연결한 ④가 적절하지 않다.

NoteBase

문 21. 다음 지문에서 설명하는 것은 무엇인가?

가. 침입탐지시스템(IDS, Intrusion Detection System)의 일종이다.
나. Rule을 이용한 침입탐지 분석 기능을 가지고 있다.
다. 네트워크상에서 실시간 트래픽 분석, 프로토콜 분석이 가능하다.

① Snort
② Sniffer
③ Strings
④ Encase

정답 1번

간단한 해설

침입탐지 기능에 **규칙 기반 분석과 실시간 네트워크 트래픽 분석**을 결합한 도구는 Snort이다. 단순한 패킷 수집뿐 아니라 규칙에 부합하는 공격 징후를 탐지한다.

핵심 풀이

가. Snort는 네트워크에서 의심스러운 활동을 탐지하는 침입탐지시스템으로 사용할 수 있다. 관찰한 패킷에서 공격 징후를 찾아 경고하는 역할을 한다.

나. Snort는 **탐지 규칙에 맞는 패킷을 찾아 경고**할 수 있다. 규칙에는 프로토콜, 주소·포트, 패킷 내용 등 탐지할 조건을 지정하므로, 단순 수집을 넘어 침입 여부를 분석한다.

다. 네트워크 트래픽을 실시간으로 살펴보고 프로토콜의 구조와 내용을 분석할 수 있다. 따라서 실시간 트래픽·프로토콜 분석이라는 단서도 Snort에 부합한다.

Sniffer는 일반적으로 네트워크 패킷을 수집·분석하는 도구를 가리킨다. 지문은 여기에 **규칙 기반 침입탐지**라는 기능까지 명시하므로 Snort가 더 정확한 식별 대상이다.

Strings는 파일에서 읽을 수 있는 문자열을 추출하는 도구이다. 네트워크 침입탐지시스템의 이름이 아니다.

Encase는 디지털 증거의 수집·분석에 사용하는 포렌식 도구이다. 실시간 규칙 기반 네트워크 침입탐지를 가리키는 지문의 대상과 구별된다.

따라서 세 단서를 모두 만족하는 것은 Snort이며, ①에 해당한다.

NoteBase

문 22. 데이터 통신에서 사용되는 통신방식에 대한 설명 중 옳은 것은 무엇인가?

① Half-duplex 방식은 한쪽에서 데이터를 보내고 난 이후, 다른 한쪽에서 데이터 전송이 가능하다.

② Full-duplex 방식은 수신측에서는 송신측으로 응답할 수 없다.

③ Half-duplex 방식은 키보드(입력)와 모니터(출력) 사이의 전송이다.

④ Full-duplex 방식은 양방향으로 송수신이 가능하나, 한 순간에는 반드시 한쪽 방향으로만 전송 가능하다.

정답 1번

간단한 해설

반이중(Half-duplex)은 양방향 통신이 가능하지만 **한 순간에는 한쪽만 송신**하므로 양쪽이 번갈아 보낸다. 양쪽이 동시에 송수신할 수 있는 전이중(Full-duplex)과 구별해야 한다.

선지별 해설

① O: 반이중은 송신 방향을 바꿀 수 있지만 양방향 동시 전송은 할 수 없다. 따라서 한쪽의 송신이 끝나 통신 경로를 넘겨받은 뒤 다른 쪽이 송신한다. 무전기에서 한 사람이 말하는 동안 다른 사람이 듣는 방식이 대표적인 예다.

② X: 전이중은 양쪽이 **동시에 송신과 수신**을 할 수 있는 방식이므로, 수신한 쪽도 상대방에게 응답할 수 있다. 한쪽 방향으로만 전송할 수 있어 역방향 응답이 불가능한 것은 단방향(Simplex) 방식에 대한 설명이다.

③ X: 입력 전용인 키보드의 데이터 입력과 출력 전용인 모니터의 화면 출력이라는 기능을 기준으로 보면 각각 한 방향의 정보 흐름, 즉 단방향 방식의 예이다. 입력 장치와 출력 장치가 있다는 사실만으로 반이중이 되지는 않는다. 반이중이려면 같은 두 통신 주체가 송신 방향을 바꾸어 **양방향으로 번갈아 전송**해야 한다.

④ X: 양방향 통신은 가능하지만 한 순간에는 한 방향으로만 전송한다는 것은 반이중의 정의이다. 전이중은 두 방향의 데이터 전송을 동시에 수행할 수 있으므로 '반드시 한쪽 방향으로만'이라는 제한이 없다.

NoteBase

문 23. Traceroute 명령은 자신의 컴퓨터가 인터넷을 통해 목적지를 찾아가면서 거치는 구간의 정보를 기록하는 유틸리티이다. 이때 ICMP 프로토콜과 IP헤더의 ( ) 필드를 사용하여 라우팅 경로를 추적한다. ( )에 들어 갈 적합한 단어는 무엇인가?

① 버전

② TOS

③ TTL

④ Checksum

정답 3번

간단한 해설

Traceroute는 **TTL 값을 조금씩 늘려** 탐사 패킷을 보내고, TTL이 소진된 지점에서 돌아오는 ICMP 메시지로 중간 라우터를 알아낸다.

빈칸별 해설

빈칸: TTL(Time To Live). IPv4 헤더의 TTL은 패킷이 네트워크 안에서 무한히 순환하지 못하도록 수명을 제한하는 필드이다. 라우터가 패킷을 전달할 때 값을 줄이며, 전달 과정에서 0이 되면 패킷을 폐기하고 보통 ICMP Time Exceeded 메시지를 송신자에게 보낸다.

경로 추적에서는 먼저 TTL을 1로 설정하여 첫 번째 라우터에서 만료되게 하고, 다음에는 2로 설정하여 그다음 라우터까지 도달하게 한다. 이처럼 TTL을 늘려 가면서 **만료 메시지를 보낸 라우터의 주소**를 확인하면 목적지까지의 경로를 순서대로 추적할 수 있다.

버전은 IP 형식의 버전, TOS는 서비스 특성, Checksum은 IPv4 헤더의 오류 검출에 관련된다. 이들은 TTL처럼 통과 가능한 구간을 제한하여 만료 지점을 바꾸는 필드가 아니다.

따라서 반복된 두 괄호에 들어갈 같은 필드는 TTL이며, ③에 해당한다.

NoteBase

문 24. 다음 중 서비스 거부 공격에 의해 직접적으로 위협받을 수 있는 정보보호의 요소는 무엇인가?

① 무결성
② 부인방지
③ 기밀성
④ 가용성

정답 4번

간단한 해설

서비스 거부 공격은 정당한 이용자가 서비스를 정상적으로 이용하지 못하게 한다. 따라서 직접 위협받는 요소는 **가용성**이다.

개념 구분

서비스 거부(DoS) 공격은 자원을 고갈시키거나 시스템·서비스의 정상 동작을 방해하여 정당한 이용자가 서비스를 이용하지 못하게 하는 공격이다. 따라서 직접적인 공격 대상은 **필요할 때 정보와 서비스를 이용할 수 있는 성질**이다.

무결성은 정보가 허가 없이 변경되거나 훼손되지 않고 정확하고 완전하게 유지되는 성질이다. 데이터를 무단으로 변조하는 공격과 구별해야 한다.

부인방지는 송신·수신 또는 특정 행위를 수행한 주체가 나중에 그 사실을 부인하지 못하도록 증거를 제공하는 것이다. 서비스 이용 가능 여부를 뜻하지 않는다.

기밀성은 허가되지 않은 주체에게 정보가 공개되지 않는 성질이다. 정보의 유출이나 도청을 막는 것과 서비스의 정상 이용을 보장하는 것은 구별된다.

가용성은 인가된 이용자가 필요할 때 정보·시스템·서비스에 접근하여 이용할 수 있는 성질이다. 서비스 거부 공격은 이 이용 가능성을 직접 방해하므로 정답은 ④이다.

NoteBase

문 25. 컴퓨터의 네트워크 연결 상태를 점검하기 위해 netstat 명령을 사용하였다. 다음 중 옳지 않은 것은 무엇인가?

① LISTENING - 연결을 위하여 접속을 대기하고 있는 상태

② CLOSED_WAIT - 완전히 종료된 상태

③ ESTABLISHED - 서로 연결된 상태

④ TIME_WAIT - 연결이 종료되었거나 다음 연결을 위해 대기하고 있는 상태

정답 2번

간단한 해설

CLOSE_WAIT는 상대방의 연결 종료 요청을 받은 뒤 로컬 응용 프로그램의 종료 처리를 기다리는 상태이다. 연결이 완전히 없어진 **CLOSED** 상태와 구별해야 한다.

선지별 해설

netstat의 TCP 상태는 연결 요청을 기다리는 단계, 연결이 성립한 단계, 연결을 종료하는 단계를 구별하여 보여준다. 종료 요청을 받았다는 사실만으로 양쪽의 종료 절차가 모두 끝난 것은 아니다.

① O: LISTENING은 다른 컴퓨터로부터 들어올 연결 요청을 기다리는 상태이다. 서버가 포트를 열어 두고 접속을 수락할 준비가 되어 있지만, 특정 상대방과의 연결이 이미 성립했다는 뜻은 아니다.

② X: 선지의 CLOSED_WAIT는 표준적으로 **CLOSE_WAIT**라고 쓰는 종료 대기 상태를 가리킨다. 상대방의 FIN을 받아 확인 응답을 보낸 뒤, 로컬 응용 프로그램이 소켓을 닫기를 기다리는 단계이므로 완전히 종료된 상태가 아니다. 연결 자체가 존재하지 않는 상태는 **CLOSED**이다.

③ O: ESTABLISHED는 TCP 연결 설정 절차가 완료되어 양쪽 사이에 연결이 성립한 상태이다. 이 상태에서 응용 프로그램의 데이터를 송수신할 수 있다.

④ O: TIME_WAIT는 연결 종료 절차 뒤에 일정 시간 상태를 유지하는 대기 단계이다. 마지막 확인 응답이 유실되었을 때 재전송에 대응하고, 이전 연결의 지연된 세그먼트가 이후 연결에 영향을 주는 것을 막는다. 선지의 다음 연결을 위한 대기는 이러한 안전한 종료 대기를 뜻하며, 새 접속 요청을 받아들이는 LISTENING과는 구별된다.

NoteBase

문 26. 다음 중 지문에서 설명하는 공격 방식과 바르게 짝지어진 것은 무엇인가?

가. 패킷을 전송할 때 출발지IP주소와 목적지IP주소를 동일하게 만들어 전송하는 공격
나. TCP 3-way handshake 과정 중 Listen 상태에서 SYN을 받은 서버가 SYN/ACK를 전달한 후 ACK를 무한정 기다리게 하는 공격
다. 공격자가 다량의 ICMP Echo Request의 출발지IP주소를 피해시스템의 IP주소로, 목적지IP주소를 Direct Broadcast IP주소로 Spoofing하여 공격

① 가: Smurf Attack, 나: SYN Flooding Attack, 다: Land Attack
② 가: SYN Flooding Attack, 나: Land Attack, 다: Smurf Attack
③ 가: Land Attack, 나: SYN Flooding Attack, 다: Smurf Attack
④ 가: SYN Flooding Attack, 나: Smurf Attack, 다: Land Attack

정답 3번

간단한 해설

출발지·목적지 IP의 동일성은 Land, **미완성 TCP 연결의 누적**은 SYN Flooding, **브로드캐스트 ICMP 응답의 집중**은 Smurf를 식별하는 단서이다.

대응 관계 해설

가. Land Attack: **출발지 IP와 목적지 IP를 피해 시스템의 주소로 같게** 설정한 패킷을 보내, 취약한 시스템의 통신 처리를 혼란시키는 공격이다. 출발지와 목적지의 동일성이 이 지문을 가르는 단서이다.

나. SYN Flooding Attack: TCP 연결은 SYN → SYN/ACK → ACK의 교환으로 성립한다. 마지막 ACK가 오지 않는 연결 요청이 대량으로 쌓이면 서버가 **연결이 완성되지 않은 상태를 유지하는 자원**을 소모한다. 지문의 '무한정'은 이런 대기 상태를 악용한다는 표현이며, 실제 개별 연결에는 일반적으로 타임아웃이 있다.

다. Smurf Attack: 출발지를 피해 시스템으로 위조한 ICMP Echo Request를 브로드캐스트 주소로 보낸다. 이를 받은 여러 호스트의 Echo Reply가 피해 시스템으로 향하면서 **응답 트래픽이 증폭되어 집중**되는 원리를 악용한다.

따라서 가는 Land Attack, 나는 SYN Flooding Attack, 다는 Smurf Attack이며, 이 대응은 ③과 일치한다.

NoteBase

문 27. 다음 중 쿠키 세션 위조 공격과 그 방지방법에 대한 설명으로 옳지 않은 것은 무엇인가?

① SSO(Single-Sign-On)를 사용하는 응용프로그램의 경우 공격자는 쿠키를 알아냄으로써 공격을 수행할 수 있다.

② 사용자 PC에 저장되는 쿠키정보는 불안전하므로 암호화하여 변조를 방지할 수 있다.

③ 세션이 비활성 상태인 동안에도 발생 가능하다.

④ 세션관리 정보를 서버 측에 저장하고 서버 측 세션을 사용하도록 구현함으로써 쿠키 세션 위조 공격을 방지할 수 있다.

정답 3번

간단한 해설

세션의 비활성을 **만료·무효화되어 서버가 인정하지 않는 상태**로 보면, 그 쿠키만으로 유효한 인증 상태를 악용할 수 없다. 사용자가 잠시 입력하지 않는 유휴 상태와는 다르다.

선지별 해설

① O: SSO를 사용하는 응용프로그램에서 인증 세션 쿠키를 확보하면, 서버가 이를 유효한 인증 정보로 받아들이는 동안 다른 사용자로 가장하는 공격을 할 수 있다. SSO라는 사실만으로 공격이 가능한 것은 아니며, **인증에 쓰이는 유효한 쿠키**가 악용되는 상황을 말한다.

② O: 클라이언트가 보관하는 쿠키의 세션관리 정보를 암호학적으로 보호하면 내용 노출과 위·변조를 방어할 수 있다. 다만 **일반적인 암호화만으로 무결성이 자동 보장되지는 않는다**. 변조를 검출하여 거부하려면 MAC이나 인증된 암호화처럼 무결성 검증을 포함한 보호가 필요하며, 이 조건을 갖춘 암호화 보호라는 취지로 이해해야 한다.

③ X: '세션이 비활성 상태인 동안에도 발생 가능하다.'에서 비활성 세션은 서버가 만료·무효화하여 더 이상 유효한 인증 상태로 인정하지 않는 경우로 구분한다. 서버가 해당 세션을 정상적으로 폐기했다면 그 세션 쿠키만으로 인증 상태를 다시 이용할 수 없다. **단순한 사용자 유휴 상태와 세션 무효화는 다르다**. 사용자가 입력하지 않는 동안에도 세션이 서버에서 유효하게 남아 있다면, 탈취한 쿠키가 악용될 수 있으므로 '활동이 없으면 안전하다'고 이해하면 안 된다.

④ O: 세션관리 정보를 서버에 보관하고 클라이언트에는 식별자만 전달하면, 클라이언트가 쿠키의 사용자 등급이나 권한 값을 고쳐 서버의 인증 상태를 바꾸는 공격을 막을 수 있다. 서버가 자신의 세션 저장소를 신뢰 기준으로 삼기 때문이다. 다만 유효한 세션 식별자 자체를 탈취해 재사용하는 공격까지 이 방식 하나로 차단하는 것은 아니므로 식별자 보호와 만료·무효화 관리도 필요하다.

NoteBase

문 28. 다음은 웹서버 로그에서 볼 수 있는 상태코드(응답코드)로 HTTP/1.1에서 정의한 것이다. 옳지 않은 것은 무엇인가? (상태코드 : 설명)

① 200 : OK

② 400 : Access Denied

③ 404 : Not Found

④ 500 : Internal Server Error

정답 2번

간단한 해설

HTTP 상태코드 400은 접근 거부가 아니라 **잘못된 요청을 뜻하는 Bad Request**이다. 요청 문법이나 메시지 형식 등 클라이언트 측 요청에 문제가 있을 때 사용한다.

선지별 해설

① O. 200 OK는 요청이 성공했음을 나타낸다. 예를 들어 GET 요청에 대한 200 응답은 요청한 자원의 표현을 정상적으로 반환하는 경우에 사용된다.

② X. 400의 설명은 **Bad Request**로, 잘못된 문법이나 메시지 형식 등 요청 자체의 문제 때문에 서버가 처리할 수 없거나 처리하지 않는 경우를 뜻한다. 요청을 이해했지만 허용하지 않는 접근 거부는 403 Forbidden과 구분해야 한다.

③ O. 404 Not Found는 서버가 요청 대상의 현재 표현을 찾지 못했음을 나타낸다. 대상의 존재를 공개하지 않으려는 경우에도 사용할 수 있으며, 코드 자체가 영구적인 삭제를 뜻하지는 않는다.

④ O. 500 Internal Server Error는 서버가 예상하지 못한 내부 상황 때문에 요청을 수행하지 못했음을 나타낸다. 클라이언트의 잘못된 요청을 뜻하는 400과 달리 **서버 측 오류**에 해당한다.

400을 Access Denied와 연결한 ②가 옳지 않은 대응이다.

NoteBase

문 29. 다음 지문에서 설명하는 공격 방법은 무엇인가?

가. 웹 서버에 명령을 실행하여 관리자 권한을 획득하는 공격 방법이다.
나. 웹 어플리케이션의 첨부파일에 대한 부적절한 신뢰와 불충분한 점검으로 인해 악의적인 공격코드가 웹 서버로 전송, 실행되는 방법이다.
다. 파일 업로드 취약점을 이용하며, 이것의 종류로는 서버 명령을 실행할 수 있는 asp, cgi, php, jsp 파일 등이 있다.

① 웹쉘(Web Shell)
② 워터링홀(Watering Hole)
③ APT(Advanced Persistent Threats)
④ Encase

정답 1번

간단한 해설

업로드된 악성 파일이 웹 서버에서 실행되어 **원격 명령 실행 통로**가 되는 것은 웹쉘이다. 파일 업로드 검사와 서버 측 실행 통제가 불충분할 때 이런 통로가 만들어질 수 있다.

NoteBase

핵심 풀이

가. 웹쉘은 웹 서버에 놓인 스크립트를 통해 외부에서 명령을 실행하거나 서버 기능을 제어하게 하는 수단이다. 지문은 이를 이용한 권한 획득을 설명한다. 실제 명령은 보통 **웹 서버 프로세스의 권한 범위**에서 실행되므로, 웹쉘이 있다는 사실만으로 관리자 권한이 자동 확보되는 것은 아니다.

나. 첨부파일을 충분히 검사하지 않으면 공격 코드가 포함된 파일이 서버에 저장될 수 있다. 그 파일이 서버에서 실행되면 단순한 첨부파일 보관 기능이 **서버 측 코드 실행 통로**로 악용된다.

다. 지문에 제시된 asp·cgi·php·jsp 파일은 서버 측에서 실행될 수 있는 파일을 가리킨다. 핵심은 확장자 자체가 아니라, 업로드된 악성 코드가 서버 설정과 실행 환경에 의해 실행되어 명령을 처리한다는 점이다.

워터링홀은 공격 대상이 자주 방문하는 웹사이트를 침해하여 방문자를 노리는 방식이다. 서버에 명령 실행용 파일을 올리는 도구 자체의 명칭은 아니다.

APT는 특정 대상을 향해 장기간 지속되는 정교한 위협·공격을 가리킨다. 웹쉘이 그 과정에서 사용될 수 있지만, 지문의 구체적인 수단은 웹쉘이다.

Encase는 디지털 증거를 수집·분석하는 포렌식 도구로, 지문에서 설명하는 공격 수단과 다르다.

따라서 파일 업로드 취약점과 서버 측 명령 실행을 설명하는 대상은 웹쉘이며, ①에 해당한다.

NoteBase

문 30. OWASP는 주로 웹에 관한 정보노출, 악성파일 및 스크립트, 보안 취약점을 연구하고 있다. '10대 웹 어플리케이션 취약점' 2013년 에디션에 속하지 않는 것은 무엇인가?

① Buffer Overflow(버퍼 오버플로우)

② Broken Authentication and Session Management(인증 및 세션 관리 취약점)

③ Cross Site Scripting(크로스 사이트 스크립팅)

④ Injection(인젝션)

정답 1번

간단한 해설

2013년판에는 인젝션, 인증 및 세션 관리 취약점, 크로스 사이트 스크립팅이 포함된다. **버퍼 오버플로우는 그 판의 독립 항목이 아니다**.

개념 구분

이 문제는 모든 보안 취약점이 아니라 **OWASP Top 10의 2013년판 목록**에 포함되는지를 묻는다. 실제 취약점이라는 사실과 해당 판의 독립 항목으로 선정되었다는 사실을 구별해야 한다.

① Buffer Overflow는 버퍼의 경계를 넘어 데이터를 기록하여 메모리를 손상시키는 등의 문제이다. 보안상 위험한 취약점이지만, 2013년판 Top 10의 독립 항목에는 포함되지 않는다.

② Broken Authentication and Session Management는 2013년판의 A2이다. 인증과 세션 관리의 결함으로 비밀번호·세션 토큰 등이 탈취되거나 다른 사용자를 사칭할 수 있는 문제를 다룬다.

③ Cross Site Scripting은 2013년판의 A3이다. 신뢰할 수 없는 입력이 안전하게 처리되지 않아 웹 페이지에 삽입되고, 피해자의 브라우저에서 악성 스크립트가 실행될 수 있는 취약점이다.

④ Injection은 2013년판의 A1이다. 신뢰할 수 없는 입력이 명령이나 질의의 일부로 해석되어 의도하지 않은 동작을 일으키는 문제이며, SQL 인젝션 등이 대표적이다.

따라서 2013년판 목록에 속하지 않는 항목은 ① Buffer Overflow이다.

NoteBase

문 31. 웹과 DB를 연동한 어플리케이션에서 SQL Injection 공격을 방어하기 위한 방법으로 옳지 않은 것은 무엇인가?

① DB 어플리케이션을 최소권한으로 구동한다.

② DB에 내장된 프로시저를 사용한다.

③ 원시 ODBC 에러를 사용자가 볼 수 있도록 코딩한다.

④ DB 테이블 이름, 컬럼 이름, SQL구조 등이 외부 HTML에 포함되어 나타나지 않도록 한다.

정답 3번

간단한 해설

원시 ODBC 오류는 테이블명이나 SQL 구문 같은 **공격에 도움이 되는 내부 정보**를 드러낼 수 있다. 사용자에게는 일반적인 오류 안내만 보여 주고, 상세 원인은 접근이 제한된 서버 로그에 기록해야 한다.

선지별 해설

① O. 애플리케이션의 DB 계정에는 업무에 필요한 최소한의 조회·변경 권한만 부여해야 한다. 불필요한 관리자 권한을 없애면 SQL Injection이 발생하더라도 접근하거나 변경할 수 있는 데이터의 범위를 제한할 수 있다.

② O. DB에 저장된 프로시저를 안전하게 작성하여 호출하는 것은 방어 방법이 된다. 입력을 SQL 문자열에 이어 붙이지 않고 **매개변수 값으로 처리**하여 명령과 데이터를 구분해야 한다. 프로시저 안에서 사용자 입력으로 동적 SQL을 조립한다면 여전히 취약할 수 있으므로, 저장 프로시저라는 이유만으로 안전한 것은 아니다.

③ X. 원시 ODBC 오류를 그대로 노출하면 DB 구조나 실행된 SQL의 일부가 드러나 공격자가 취약점을 파악하는 데 이용할 수 있다. **외부에는 일반 오류 메시지**를 제공하고, 분석에 필요한 상세 오류는 권한이 제한된 내부 로그로 남겨야 한다.

④ O. 외부로 전달되는 HTML에 테이블명·컬럼명·SQL 구조 같은 불필요한 내부 정보를 넣지 않으면 공격자에게 단서를 제공하는 일을 줄일 수 있다. 다만 정보 비공개만으로 주입 취약점이 사라지지는 않으므로 매개변수화된 쿼리 같은 근본 대책과 함께 적용해야 한다.

내부 오류를 사용자에게 노출하도록 하는 ③이 방어 방법으로 옳지 않다.

NoteBase

문 32. 다음 지문에서 설명하는 DB보안 요구 사항은 무엇인가?

가. 기밀이 아닌 데이터로부터 기밀 정보를 얻어내는 가능성을 의미한다.
나. DB데이터는 상호연관 가능성이 있어, 데이터에 직접 접근하지 않고도 가용한 데이터 값을 이용할 수 있다.
다. 통계적인 데이터 값으로부터 개별적인 데이터 항목에 대한 정보를 추적하지 못하도록 하는 것을 의미한다.

① 추론 방지
② 데이터 무결성
③ 감사 기능
④ 사용자 인증

정답 1번

간단한 해설

직접 공개하지 않은 민감한 정보도 공개된 값이나 통계 결과를 결합하면 알아낼 수 있다. **허용된 데이터에서 비밀 정보를 간접적으로 도출하지 못하게 하는 것**이 추론 방지이다.

NoteBase

핵심 풀이

DB 보안에서 추론은 직접 접근할 수 없는 비밀 정보를, 접근 가능한 데이터의 관계나 통계 결과로부터 알아내는 것이다. 추론 방지는 단순히 비밀 열을 숨기는 데 그치지 않고 **여러 공개 결과를 결합했을 때 드러나는 정보**까지 통제하는 요구 사항이다.

가. 기밀이 아닌 데이터로부터 기밀 정보를 얻는 가능성: 개별 조회 결과는 공개해도 되는 값이어도, 서로 결합하면 공개하지 않은 사실을 드러낼 수 있다. 이 간접적인 정보 도출이 추론의 위험이며, 이를 막는 것이 질문에서 찾는 보안 요구 사항이다.

나. 데이터의 상호연관성: 표 사이의 관계나 알려진 속성을 이용하면 보호 대상 레코드를 직접 읽지 않고도 그 값을 유추할 수 있다. 따라서 특정 데이터에 대한 직접 접근 권한만 제한했다고 해서 모든 정보 노출이 막히는 것은 아니다.

다. 통계값에서 개별 항목을 추적하지 못하게 함: 예를 들어 집단 전체의 합계와 그중 한 명만 뺀 집단의 합계를 모두 알면, 두 합계의 차이로 그 한 명의 값을 계산할 수 있다. 집계 결과의 공개 범위나 서로 연관된 질의를 통제하는 등 이러한 **통계적 추론을 통한 개별 정보 노출**을 막는 것이 핵심이다.

데이터 무결성은 데이터가 부당하게 변경·손상되지 않고 정확성을 유지하도록 하는 요구이다. 이 지문은 값의 변경이 아니라 보호된 정보의 간접 노출을 다룬다.

감사 기능은 누가 언제 어떤 데이터를 조회하거나 변경했는지 등의 기록을 남겨 사후 추적과 점검을 가능하게 한다. 기록을 남기는 기능 자체가 추론 방지와 같은 뜻은 아니다.

사용자 인증은 접근을 요청하는 사용자가 주장하는 신원과 일치하는지 확인한다. 정상적으로 인증된 사용자도 허용된 질의 결과를 조합하여 정보를 추론할 수 있으므로, 인증만으로 지문의 위험을 해결하지는 못한다.

가·나는 추론의 위험을, 다는 이를 막아야 한다는 요구를 설명하므로 정답은 **추론 방지인 ①**이다.

NoteBase

문 33. 다음 지문에서 설명하는 시스템은 무엇인가?

가. 공격성향이 있는 자들을 중요한 시스템으로부터 다른 곳으로 끌어내도록 설계된 유도시스템이다.
나. 공격자의 동작에 관한 정보를 수집한다.
다. 관리자가 반응할 수 있도록 공격자로 하여금 시스템에 충분히 오랜 시간동안 머무르도록 유도한다.

① 라디어스(RADIUS)

② 허니팟(Honeypot)

③ 방화벽(Firewall)

④ AAA(Authentication Authorization Accounting)

정답 2번

간단한 해설

허니팟은 **공격자를 유인하여 행동을 관찰·기록**하는 시스템이다. 실제 보호 대상으로 향하는 관심을 돌리고 공격 정보를 수집하며 대응 시간을 확보하는 데 목적이 있다.

NoteBase

핵심 풀이

가. 허니팟은 공격자가 관심을 가질 만한 시스템이나 자원을 마련하여 **실제 보호 대상에서 공격자의 관심을 돌리는 유인 장치**이다. 중요한 운영 시스템과 구별된 대상으로 공격을 끌어들이는 것이 핵심이다.

나. 유인된 공격자의 접속, 사용 명령, 시도한 공격 등을 관찰·기록하면 공격 수법과 행동에 관한 정보를 얻을 수 있다. 허니팟은 이런 분석 자료를 수집하는 데 활용된다.

다. 공격자가 유인 환경에서 활동하도록 하여 관리자가 탐지·분석하고 대응할 시간을 확보하려는 목적도 있다. 다만 공격자를 반드시 붙잡아 두거나 모든 공격을 막는다는 뜻은 아니다.

라디어스는 네트워크 접속자의 인증·인가 정보를 교환하는 프로토콜이다. 접속을 허용할 사용자를 확인하는 기능은 공격자를 유인하는 기능과 다르다.

방화벽은 보안 정책에 따라 통신을 허용하거나 차단한다. **통신을 통제하는 방화벽**과 **공격자를 유인·관찰하는 허니팟**은 주된 역할이 다르다.

AAA는 인증, 인가, 계정 관리의 세 기능을 묶은 개념이다. 각각 사용자 확인, 허용 권한 결정, 이용 내역 기록을 뜻하며, 공격자 유도 시스템의 명칭은 아니다.

따라서 공격자 유인·행동 정보 수집·대응 시간 확보를 설명하는 시스템은 허니팟이며, ②에 해당한다.

NoteBase

문 34. 다음 중 공격 명칭과 공격에 대한 설명이 바르게 짝지어진 것은 무엇인가?

가. ARP Spoofing - IP주소를 위·변조하는 공격
나. XSS(Cross Site Scripting) - 게시물에 실행코드와 태그의 업로드가 규제되지 않는 경우 이를 악용하여 열람한 타 사용자의 PC로부터 정보를 유출할 수 있는 공격
다. MITM(Man-In-The-Middle) 공격 - 통신하고 있는 두 당사자 사이에 끼어들어 당사자들이 교환하는 정보를 자기 것과 바꾸어 버림으로써 들키지 않고 도청을 하거나 통신 내용을 바꾸는 공격

① 가, 나
② 가, 다
③ 나, 다
④ 가, 나, 다

정답 3번

간단한 해설

ARP 스푸핑은 IP 주소와 MAC 주소의 대응 관계를 속이는 공격이다. 게시물을 열람한 사용자의 브라우저에서 악성 코드를 실행시키는 것은 XSS이고, 통신 당사자 사이에서 정보를 가로채거나 바꾸는 것은 MITM 공격이다.

보기별 해설

공격 이름을 구별할 때는 무엇을 위조하는지, 악성 코드가 어디에서 실행되는지, 공격자가 통신 경로의 어디에 개입하는지를 확인한다.

가. X: ARP는 같은 네트워크에서 IP 주소에 대응하는 MAC 주소를 알아내는 데 사용된다. ARP 스푸핑은 거짓 ARP 정보를 보내 피해자의 ARP 캐시에 **정상 IP 주소와 공격자의 MAC 주소를 잘못 연결**시키는 공격이다. IP 패킷의 출발지 IP 주소를 위조하여 다른 호스트인 것처럼 보이게 하는 IP 스푸핑과 구별해야 한다.

나. O: XSS는 웹 페이지에 삽입된 악성 스크립트가 **페이지를 열람한 사용자의 브라우저에서 실행**되도록 하는 공격이다. 게시물에 저장된 코드가 다른 사용자의 열람 때 실행되는 경우는 저장형 XSS에 해당한다. 브라우저가 접근할 수 있는 세션 정보나 페이지의 민감한 정보를 유출할 수 있으므로 제시된 설명과 연결된다.

다. O: MITM 공격은 두 통신 당사자 사이에 개입하여 각 당사자에게 정상 상대방과 통신하는 것처럼 보이게 하는 공격이다. 공격자는 중간에서 메시지를 전달하면서 내용을 엿보거나 바꿀 수 있다. 따라서 **통신 경로 중간에서의 도청·변조**라는 설명이 부합한다.

바르게 짝지어진 보기는 나와 다이므로, 이 조합을 제시한 ③과 연결된다.

NoteBase

문 35. 다음 중 공격기법과 그에 대한 설명으로 옳은 것은 무엇인가?

① Smurf Attack : IP Broadcast Address로 전송된 ICMP 패킷에 대해 응답하지 않도록 시스템을 설정하여 방어할 수 있다.

② Heap Spraying : 아이디와 패스워드 같이 사용자의 입력이 요구되는 정보를 프로그램 소스에 기록하여 고정시키는 방식이다.

③ Backdoor : 조직 내에 신뢰할 만한 발신인으로 위장해 ID 및 패스워드 정보를 요구하는 공격이다.

④ CSRF : 다른 사람의 세션 상태를 훔치거나 도용하여 액세스하는 해킹 기법을 말한다.

정답 1번

간단한 해설

Smurf 공격은 브로드캐스트에 대한 다수의 ICMP 응답을 피해자에게 집중시키는 방식이다. **브로드캐스트 ICMP 요청에 응답하지 않으면** 응답 증폭에 가담하는 것을 막을 수 있다.

선지별 해설

① O. Smurf 공격은 출발지 주소를 피해자의 IP 주소로 위조한 ICMP Echo Request를 브로드캐스트 주소로 보내 다수 호스트의 응답이 피해자에게 집중되게 한다. 따라서 **브로드캐스트로 들어온 ICMP Echo Request에 응답하지 않도록** 설정하면 자신의 시스템이 응답 증폭에 이용되는 것을 막을 수 있다.

② X. 아이디·패스워드 같은 값을 소스 코드에 고정해 넣는 것은 하드코딩에 해당한다. Heap Spraying은 힙 메모리에 공격자가 원하는 코드나 데이터를 반복적으로 배치하여, 취약점 악용 시 그 영역에 도달할 가능성을 높이는 기법이다. 인증정보를 소스에 고정하는 방식과는 다르다.

③ X. 신뢰할 만한 발신인을 사칭해 인증정보를 요구하는 설명은 피싱에 해당하며, 특정 조직이나 대상을 겨냥하면 스피어 피싱의 성격을 갖는다. Backdoor는 정상적인 인증·접근 통제를 우회해 시스템에 접근할 수 있게 하는 숨겨진 통로나 기능이다.

④ X. 다른 사람의 세션을 탈취·도용하여 그 사람처럼 접근하는 것은 세션 하이재킹이다. CSRF는 인증된 사용자의 브라우저가 그 사용자의 의도와 다른 요청을 보내도록 유도하는 공격이다. 브라우저에 이미 있는 인증 상태를 악용하므로 공격자가 세션 식별자를 직접 훔쳐야만 가능한 것은 아니다.

이와 같이 공격기법과 설명이 올바르게 연결된 선지는 ①이다.

NoteBase

문 36. 최근 사이버범죄자들은 인터넷 접속 시 추적을 피하기 위해 VPN(Virtual Private Network)서비스를 이용하고 있다. 다음 중 VPN에서 사용하는 프로토콜이 아닌 것은 무엇인가?

① PPTP(Point-to-Point Tunneling Protocol)

② L2TP(Layer 2 Tunneling Protocol)

③ PGP(Pretty Good Privacy)

④ IPSec(Internet Protocol Security)

정답 3번

간단한 해설

PGP는 전자우편이나 파일의 **내용을 암호화하고 전자서명하는 기술**이다. 공중망 위에 가상 사설 통신 경로를 만드는 VPN 프로토콜과는 용도가 다르다.

개념 구분

VPN은 공중망을 통해 사설 통신 경로를 구성하며, 터널링과 필요한 보안 기능을 조합해 사용한다. 이 문제는 암호 기술을 사용하는지 여부가 아니라 **VPN 통신 경로 구성에 쓰이는 기술인지**를 구분해야 한다.

PPTP는 PPP 프레임을 IP 네트워크 위에서 터널링하는 프로토콜로, 원격 접속 VPN 구성에 사용되어 왔다.

L2TP도 PPP 프레임을 터널로 전달하는 프로토콜이다. 자체 터널링만으로 데이터 암호화까지 제공하는 것은 아니므로 보안을 위해 IPsec과 결합해 사용한다.

PGP는 메시지나 파일의 암호화·전자서명에 쓰인다. 공개키 암호와 대칭키 암호 등을 활용하여 내용의 기밀성과 발신자 확인·무결성 검증을 제공하지만, 그 자체가 VPN 터널을 만드는 프로토콜은 아니다.

IPsec은 IP 계층에서 통신을 보호하는 프로토콜 체계이다. 인증·무결성 검증과 암호화 등의 기능을 제공하며, 터널 모드 등을 이용해 VPN을 구성할 수 있다.

따라서 VPN용 프로토콜에 해당하지 않는 것은 ③ PGP이다.

NoteBase

문 37. 다음 지문에서 설명하는 공간은 무엇인가?

저장매체의 물리적인 구조와 논리적인 구조의 차이로 발생하는 낭비 공간으로, 물리적으로 할당된 공간이지만 논리적으로는 사용할 수 없는 공간을 말한다. 램, 드라이브, 파일시스템, 볼륨 등에 나타난다.

① 클러스터(Cluster)

② 파티션(Partition)

③ 섹터(Sector)

④ 슬랙(Slack)

정답 4번

간단한 해설

할당된 저장 공간 중 논리적 데이터가 채우지 못하고 남긴 부분을 슬랙 공간이라고 한다. 파일의 실제 끝과 마지막으로 할당된 저장 단위의 끝이 일치하지 않을 때 생기는 여유 공간이 대표적이다.

NoteBase

개념 구분

지문의 핵심은 저장 공간이 할당되어 있다는 사실과, 그 공간 전체가 논리적 데이터로 사용되지는 않는다는 사실의 차이이다. **할당 범위와 실제 사용 범위 사이에 남는 틈**을 슬랙 공간이라고 한다.

슬랙(Slack): 대표적으로 파일 시스템이 클러스터 단위로 공간을 할당할 때, 마지막 클러스터를 파일 내용이 끝까지 채우지 못하면 남는 부분이 파일 슬랙이 된다. 이 부분은 현재 파일의 논리적 내용에 포함되지 않으므로 일반적인 파일 읽기로는 파일 데이터처럼 반환되지 않는다. 그렇다고 물리적으로 존재하지 않거나 포렌식 도구로도 전혀 조사할 수 없다는 뜻은 아니다.

지문에 나열된 램·드라이브·파일시스템·볼륨 관련 슬랙은 어떤 저장 구조의 경계에서 여유 부분이 생기는지를 구분하는 맥락이다. 이 문제에서는 세부 종류보다 **물리적 공간과 논리적 사용 범위의 불일치**라는 공통 특징을 잡는 것이 중요하다.

클러스터(Cluster): 파일 시스템이 파일에 공간을 할당할 때 사용하는 단위로, 보통 여러 섹터로 구성된다. 클러스터 자체는 낭비 공간의 이름이 아니며, 마지막 클러스터 안에 슬랙이 생길 수 있다.

파티션(Partition): 저장장치를 논리적으로 나눈 영역이다. 하나의 영역을 구획한 것을 뜻하므로, 할당되었지만 내용으로 채우지 못한 여유 부분을 뜻하는 슬랙과 다르다.

섹터(Sector): 저장장치의 주소 지정이나 입출력에 쓰이는 작은 저장 단위이다. 섹터는 공간을 나누는 단위의 이름이며, 그 단위 내부나 경계에 남은 여유 공간 자체를 뜻하지 않는다.

따라서 지문이 설명하는 공간은 **슬랙인 ④**이다.

NoteBase

문 38. 다음 지문에서 설명하는 포렌식 도구는 무엇인가?

가. Guidance Software Inc.가 사법기관 요구사항에 바탕을 두고 개발한 컴퓨터 증거분석용 소프트웨어이다.
나. 컴퓨터 관련 수사에서 디지털 증거의 획득과 분석 기능을 제공하며, 미국에서 1990년대 후반부터 600여개 사법기관에서 컴퓨터 관련 범죄수사에 활용되고 있으며, 미국 법원이 증거능력을 인정하는 독립적인 솔루션이다.
다. Windows 환경에서 증거원본 미디어에 어떠한 영향을 미치지 않으면서도 '미리보기', '증거사본작성', '분석', '결과보고'에 이르는 전자증거조사의 모든 과정을 수행할 수 있다.

① Wireshark
② Encase
③ KICS
④ IDA

정답 2번

간단한 해설

Guidance Software가 개발하고 **디지털 증거의 획득·분석·보고**를 지원하는 도구는 Encase이다. 원본 보존을 전제로 증거사본을 작성하고 조사하는 기능이 핵심 단서이다.

NoteBase

핵심 풀이

가. Encase는 Guidance Software가 개발한 컴퓨터 증거 분석 도구이다. **개발사와 디지털 증거 분석 목적**이라는 조합이 도구를 식별하는 직접적인 단서이다.

나. Encase는 수사에 필요한 디지털 증거를 획득하고 분석하는 기능을 제공한다. 지문의 사법기관 활용 사례와 법정 증거 관련 설명은 이러한 포렌식 활용 목적을 강조하는 단서이며, 제시된 기관 수를 현재의 이용 규모로 해석하지 않는다.

다. 미리보기로 조사 대상을 확인하고, 증거사본을 만든 뒤 내용을 분석하여 결과를 보고하는 과정을 지원한다. **원본을 보존하면서 사본을 분석**하는 것이 핵심이며, 원본 변경 방지는 적절한 쓰기 방지와 취득 절차를 함께 적용해야 한다.

Wireshark는 네트워크 패킷을 수집하고 프로토콜을 분석하는 도구이다. 지문의 개발사와 저장매체 증거 조사 전 과정이라는 설명에 해당하지 않는다.

KICS는 형사사법정보시스템으로, 형사사법 업무와 정보를 처리하는 시스템이다. 저장매체에서 디지털 증거를 획득·분석하는 해당 제품의 명칭은 아니다.

IDA는 실행 파일 등의 기계어 코드를 분석하는 디스어셈블러이다. 프로그램 역분석에 활용되지만, 지문의 개발사와 포렌식 조사 기능을 가진 도구는 Encase이다.

따라서 지문이 설명하는 포렌식 도구는 Encase이며, ②에 해당한다.

NoteBase

문 39. 다음은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제71조(벌칙) 제1항의 각 호 내용 중 일부를 나열한 것이다. 실제 내용과 다른 것은 무엇인가?

① 이용자의 동의를 받지 아니하고 개인정보를 수집한 자

② 정보통신망에 침입한 자

③ 정보통신망에 장애가 발생하게 한 자

④ 타인의 정보를 훼손하거나 타인의 비밀을 판매 또는 도용한 자

정답 4번

간단한 해설

당시 제71조 제1항은 타인의 정보를 훼손하거나 타인의 비밀을 **침해·도용 또는 누설**한 행위를 규정하였다. 선지의 **판매**는 해당 호에 열거된 법문과 다르다.

선지별 해설

이 문항은 2017년 당시 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제71조 제1항에 열거된 처벌 대상의 문구를 묻는다. 실제 행위의 처벌 여부를 일반적으로 판단하는 문제와 법문에 사용된 표현을 대조하는 문제를 구별해야 한다.

① O: 당시 제71조 제1항 제1호는 제22조 제1항을 위반하여 이용자의 동의 없이 개인정보를 수집한 자를 규정하였다. **동의가 필요한 개인정보 수집에서 동의를 받지 않은 경우**가 핵심이다. 이 선지는 그 조문의 처벌 대상을 요약한 것이다.

② O: 당시 제71조 제1항 제9호는 제48조 제1항을 위반하여 정보통신망에 침입한 자를 규정하였다. 정당한 접근권한 없이 접속하거나 허용된 접근권한을 넘어 침입하는 행위가 이에 해당하므로, 제시된 문구는 해당 호의 내용과 연결된다.

③ O: 당시 제71조 제1항 제10호는 제48조 제3항을 위반하여 정보통신망에 장애가 발생하게 한 자를 규정하였다. 단순히 장애가 발생한 모든 경우를 뜻하는 것은 아니며, 정보통신망의 안정적 운영을 방해할 목적으로 대량의 신호를 보내는 등 법이 금지한 방법으로 장애를 일으키는 행위가 대상이다.

④ X: 당시 제71조 제1항 제11호의 표현은 타인의 정보를 훼손하거나 타인의 비밀을 **침해·도용 또는 누설**한 자이다. 선지의 '판매 또는 도용'은 법문과 일치하지 않는다. 비밀을 판매하는 구체적 행위가 별도로 누설 등에 해당할 수 있는지와 무관하게, 이 문항에서는 열거된 행위의 정확한 문구가 판단 기준이다.

NoteBase

문 40. 다음은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」상 정보통신망에 유통되어서는 안 되는 불법정보 관련 조항을 나열한 것이다. 실제 내용과 다른 것은 무엇인가?

① 음란한 부호·문언·음향·화상 또는 영상을 배포·판매·임대하거나 공공연하게 전시하는 내용의 정보

② 법령에 따라 금지되는 사행행위에 해당하는 내용의 정보

③ 사람을 비방할 목적으로 공공연하게 사실이나 거짓의 사실을 드러내어 타인을 모욕하는 내용의 정보

④ 공포심이나 불안감을 유발하는 부호·문언·음향·화상 또는 영상을 반복적으로 상대방에게 도달하도록 하는 내용의 정보

정답 3번

간단한 해설

출제 당시 해당 조항은 비방할 목적으로 사실이나 거짓 사실을 드러내어 **타인의 명예를 훼손하는 정보**를 규정했다. 이를 '타인을 모욕하는 정보'로 바꾼 표현은 조문과 다르다.

선지별 해설

이 문제는 출제 당시 정보통신망법 제44조의7 제1항에 열거된 불법정보의 문구를 묻는다. 각 정보의 일반적인 위법성 여부를 새로 판단하는 문제가 아니라 조항에 적힌 내용과의 일치를 확인해야 한다.

① O. 제1호는 음란한 부호·문언·음향·화상·영상을 배포·판매·임대하거나 공개적으로 전시하는 내용의 정보를 대상으로 한다. 선지는 정보의 음란성과 유통·전시 형태를 조문대로 제시했다.

② O. 제6호는 법령이 금지하는 사행행위에 해당하는 정보를 대상으로 한다. 모든 오락 정보를 뜻하는 것이 아니라 **법령에 따라 금지되는 사행행위**라는 한정이 중요하다.

③ X. 제2호의 해당 표현은 '타인을 모욕하는'이 아니라 **'타인의 명예를 훼손하는'**이다. 당시 조문은 사람을 비방할 목적, 공공연한 사실 또는 거짓 사실의 제시, 타인의 명예 훼손을 연결하고 있다. 따라서 마지막 행위 유형을 모욕으로 바꾼 선지는 조문과 다르다.

④ O. 제3호는 공포심이나 불안감을 일으키는 부호·문언·음향·화상·영상이 상대방에게 반복적으로 도달하도록 하는 내용의 정보를 대상으로 한다. 공포·불안 유발과 반복적인 도달이라는 요소가 모두 제시되어 있다.

따라서 실제 조항의 내용과 다른 선지는 ③이다. 이는 해당 조문의 문구를 구별한 것이며, 모욕적인 정보를 유통하는 행위가 언제나 적법하다는 뜻은 아니다.

NoteBase